Community of Cooperation

Security Checklist

KoGe Association, Learning Group Good Governance

December 2020

Explanation - *This Checklist consists of two parts:*

1) ***Recommended Basic Security Standards:*** *The recommended basic security standards serve to give NGOs an overview of what they should at least have to enhance their security. These points can be implemented in a 2-12 months time frame.*

2.) ***Detailed Security Checklist:*** *For NGOs interested in taking it further, the detailed security checklist provides further information. The points mentioned in the basic list are marked bold in the detailed list. You can either fill out the first or second list, as the Detailed Security Lists includes the Recommended Basic Security Standards.*

[This checklist is based on the Guide Book "Security Risk Management: a basic guide for smaller NGOs" by EISF and ACT Alliance's security documents.]

1) Recommended Basic Security Standards	Yes	Partially	No
a) A ***security policy*** *is in place.*			
b) ***Country security plans*** *exist for each country and are regularly updated with partners.*			
c) ***Pre departure briefings*** *(incl. fillling in travel form) take place before each trip.*			
d) Each employee/volunteer has ***travel insurance*** *provided by the organisation.*			
e) An ***Incidents reporting form*** *are provided and filled out when a security incident occurs.*			
f) A ***crisis management structure*** *is in place (e.g. communication and emergency aid in case an incident occurs)*			

2) Detailed Security Checklist			
Governance and accountability	**Yes**	**Partially**	**No**
A suitable security risk management structure for the organisation is in place to enable objectives to be met and ensure there is a clear understanding of roles and responsibilities.			
A Security Focal Point (SFP) has been identified to support the development and implementation of the security risk management framework.			
Each job descriptions and Terms of Reference outline the security risk management roles and responsibilities asscoiated with this position or activity.			
Policy and principles	**Yes**	**Partially**	**No**
A security policy is in place that reflects the organisation's principles and approach to security. clearly outlines the organisation's risk attitude, security risk management structure and the security responsibilities of individual staff and those allocated specific security roles.			
Operations and programmes	**Yes**	**Partially**	**No**
A simple security risk assessment process is in place that identifies key risks in a particular country or location together with partners and outlines the control measures in place to manage these risks and summarizes it in country security plans.			
Partners are aware of their security responsibilities.			
Travel management and support	**Yes**	**Partially**	**No**
Travel risk assessments are made and approved for all occasions of staff travel to higher risk destinations, or where the nature of the visit raises security concerns.			
The organisation has specific international travel security procedures for travelling staff, consultants and visitors. These should clarify roles and responsibilities, training and briefings, travel monitoring, authorisations and emergency procedures.			
It is ensured that all staff, consultants and visitors travelling to higher risk contexts receive a pre-departure security briefing specific to the country or area they are travelling to, and sign that they have received it. If possibley, a briefing is also made by the partner in the country.			
Appropriate check-in procedures for travelling staff are in place (e.g. communication once daily) in order to monitor their movements.			
All staff, including consultants, have adequate insurance cover while travelling to and working in the field, and that all staff are fully informed of their insurance provisions.			
A security debriefing takes place after a trip.			

Awareness and capacity building	**Yes**	**Partially**	**No**
All staff receives a security induction which covers the organisation's security policy and approach, and responsibilities within the organisation (min. online, specialized trainings e.g. HEAT for those in the most difficult circumstances)			
Incident monitoring	**Yes**	**Partially**	**No**
Incident reporting procedures and reporting formats are in place and staff know what needs to be reported and how.			
Reported incidents are recorded in a system and analyzed regularly to identify strategies of prevention.			
Crisis management	**Yes**	**Partially**	**No**
A crisis management structure is in place (incl. communication plan) to coordinate and manage the organisation's response to incidents			
Develop a Crisis Management Plan which outlines the roles and functions of key staff, clarifies decision-making authority, and highlights the key response procedures for crisis situations.			
A network of contacts (medical, psychological, legal) is established to assist in case of crisis.			
Employees are able to contact an external service to talk about what they have experienced.			
Security collaboration and networks	**Yes**	**Partially**	**No**
The organisation is part of (an) inter-agency security forum/network (e.g. ACT Alliance) in order to strengthen information-sharing and security collaboration.			
Compliance and effectiveness monitoring	**Yes**	**Partially**	**No**
Managers and country representatives are provided with a security risk management checklist to help them assess compliance with security policies and minimum requirements.			
Regular country/programme security audits are conducted, especially for activities in high-risk countries.			
The organisation's security risk management approach and framework is regularly reviewed.			
Supporting resources	**Yes**	**Partially**	**No**
A range of guidance, tools and templates as part of a security library are available to assist managers and staff in managing security risks.			